

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

This Page Blank (uspto)

ABSTRACTED-PUB-NO: JP07202884A

BASIC-ABSTRACT:

The codec decodes the input individual information (152) using master key (Kmi). After decoding, the work key (kw) is stored. Another code

decoder (103) uses this work key and carries out decoding of the input common information (151). A PN signal generator (107) uses the a
scramble key (KS) and generates PN signal.

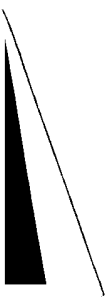
A descrambler (106) uses the PN signal and descrambler input data (150). A time information memory and timer (109), stores the updating
time information included in the decoded individual information. The power supply (125) controlled by a power supply control unit (121) is
switched ON, for execution of the above operations,

ADVANTAGE - Updates code key reliably simply, and efficiently.

CHOSEN-DRAWING: Dwg.3/4

TITLE-TERMS: CODEC TRANSCEIVER TRANSMIT INFORMATION DECODE
FIRST CODEC UPDATE INFORMATION ENCIPHER SECOND DECODE

This Page Blank (uspto)



【特許請求の範囲】

【請求項 1】 伝送すべき情報を発生する第 1 の発生手段と、

前記情報を暗号化する暗号鍵と、前記暗号鍵を更新する更新情報を発生する第 2 の発生手段と、

前記第 2 の発生手段により発生された前記暗号鍵に対応して、前記第 1 の発生手段が発生する情報を暗号化する第 1 の暗号化手段と、

前記暗号鍵と更新情報を暗号化する第 2 の暗号化手段と、

前記第 1 の暗号化手段により暗号化された情報、並びに前記第 2 の暗号化手段により暗号化された前記暗号鍵と更新情報を伝送する伝送手段とを備えることを特徴とする送信装置。

【請求項 2】 所定のタイミングで更新される暗号鍵を用いて、伝送された情報、前記暗号鍵、および前記暗号鍵の更新情報を受信する受信装置において、

前記更新情報を記憶する第 1 の記憶手段と、

前記第 1 の記憶手段に記憶された前記更新情報に基づき、電源を制御する制御手段と前記更新情報手段に基づいて更新される前記暗号鍵を記憶する第 2 の記憶手段と、

前記第 2 の記憶手段に記憶された前記記憶鍵に基づいて前記情報を復号する復号手段とを備えたことを特徴とする受信装置。

【請求項 3】 前記更新情報は、前記暗号鍵を更新する更新開始時刻を含み、

前記制御手段は、前記更新開始時刻に、前記電源を一定時間オンすることを特徴とする請求項 2 に記載の受信装置。

【請求項 4】 前記更新情報は、前記暗号鍵を更新する更新開始時刻及び前記暗号鍵の更新期間を含み、

前記制御手段は、前記更新開始時刻に前記電源をオンさせるとともに、前記更新期間に対応する時間経過後に前記電源をオフさせることを特徴とする請求項 2 に記載の受信装置。

【請求項 5】 前記更新情報は、前記暗号鍵を更新する更新開始時刻及び前記暗号鍵の更新終了時刻を含み、

前記制御手段は、前記更新開始時刻に前記電源をオンさせるとともに、前記更新終了時刻に前記電源をオフさせることを特徴とする請求項 2 に記載の受信装置。

【発明の詳細な説明】

【 0 0 0 1 】

【産業上の利用分野】本発明は、例えば有料放送において使用されるワーク鍵を自動更新する有料放送受信装置に用いて好適な送信装置および受信装置に関する。

【 0 0 0 2 】

【従来の技術】従来より、有料放送で用いられる暗号は、通常階層構造になっており、複数の鍵を利用して暗号化している。さらにこの鍵が、試行錯誤的に検査して

順次発見されないように、送信側で周期的に鍵の更新が行われている。

【 0 0 0 3 】従来の有料衛星放送方式における鍵の階層構成を、図 4 を用いて説明する。図 4 に示すように、従来の階層構成の鍵は、3 重の鍵（スクランブル鍵 K_S、ワーク鍵 K_W、マスター鍵 K_Mi）で構成されている。まず、エンコーダである送出装置 210 側では、図示しないデータ送出器からのデータを、スクランブラ 201 で共通情報であるスクランブル鍵 K_S によりスクランブルして送出し、デコーダである受信装置 220 側でデスクランブラ 205 によりデスクランブルする。このとき、後述するように、受信契約が有効な場合においてのみデスクランブルができるようになっている。

【 0 0 0 4 】スクランブラ 201 に入力されるスクランブル鍵 K_S は、非常に短い周期（たとえば 1 秒）で更新されており、読取されないように、比較的更新周期の長いワーク鍵 K_W を用いて暗号器 202 で暗号化され、受信装置 220 に送信される。ここで、送出装置 210 は、契約者に届けられたデコーダである受信装置 220 毎に付けられた個々の ID と、それに対応したマスター鍵 K_Mi を記憶部 204 にあらかじめ記憶している。そして各個人に割り当てられるワーク鍵 K_W は、各デコーダ個々のマスター鍵 K_Mi を用いて暗号器 203 で暗号化され受信装置 220 に送信される。

【 0 0 0 5 】デコーダである受信装置 220 では、この個別に送信された暗号器 203 の出力である個別情報内のワーク鍵 K_W を、記憶部 208 に記憶されている各デコーダ個々のマスター鍵 K_Mi を用いて暗号復号器 207 でデコードし、記憶する。そして、記憶されたワーク鍵 K_W で、暗号器 202 の出力である共通情報内のスクランブル鍵 K_S をデコードし、記憶する。記憶したスクランブル鍵 K_S で、スクランブラ 201 からの出力情報をデスクランブラ 205 でデスクランブルする。このように、受信契約が有効な場合（マスター鍵 K_Mi、ワーク鍵 K_W、およびスクランブル鍵 K_S が、正しいものである場合）にだけ、受信（デスクランブル）ができるようになっている。そして、復号されたデータは図示しないサービスデコーダへ出力される。

【 0 0 0 6 】各個人個々のワーク鍵 K_W をデコーダ個々のマスター鍵 K_Mi で暗号化して、所定のタイミングで送信（更新）する場合、更新周期の間に次のワーク鍵を配送すれば良いわけだが、更新周期の長さを大きく取ること、加入者の個別情報をその分だけ多く送信できるため、加入者の数も多くできる。そこで現在、例えば J S B（日本衛星放送）では、ワーク鍵 K_W の更新周期は 1 年とされている。その更新時にはデコーダが電源オンの状態、すなわち J S B を視聴している必要があるため、現在ではダイレクトメールや告知放送という形で更新時を知らせ、加入者に電源をオンさせるようになっている。また一回の伝送で視聴者がワーク鍵を受け取ること

ができるとは限らないために、何度か送るようにしており、それでも更新されない場合、または、クレームがきたとき、は個々に送信するなどの手段で対処している。

【 0 0 0 7 】

【発明が解決しようとする課題】しかしながら、上述したように、従来のワーク鍵の更新方法は、ダイレクトメールや告知放送など人手を介して行う必要があり、加入者が増加すればするほど、手続きや管理は複雑になるという問題がある。また、加入者にデコーダの電源をオンにすることを任せているために、当然ながら電源をオンせず

10

にワーク鍵が更新されないような事が生じる虞がある。実際、例えば現行のBS有料放送においては約1%のデコーダが更新不可となっている。

【 0 0 0 8 】さらに、現在はサービス（有料番組）の数が少ないためトラブルも少ないが、今後衛星データ放送等で多くのサービスが提供されると、それぞれのサービスにワーク鍵が必要で、その更新のためのトラブルも増加するものと考えられる。さらにまた、加入者がワーク鍵を確実に更新させるために、装置の電源スイッチをオンし続ける可能性があり、無駄な電力消費をする虞もある。

20

【 0 0 0 9 】本発明は上記事情に鑑みてなされたものであり、簡単かつ確実に暗号鍵を効率的に更新できる送信装置受信装置を提供することを目的とする。

【 0 0 1 0 】

【課題を解決するための手段】本発明の送信装置は、伝送すべき情報としてのスクランブル鍵KSを含む共通情報を発生する第1の発生手段としての共通情報発生回路3と、スクランブル鍵KSを暗号化する暗号鍵としてのワーク鍵KWと、ワーク鍵KWを更新する更新情報としての個別情報を発生する第2の発生手段としての個別情報発生回路5と、個別情報発生回路5により発生されたワーク鍵KWに対応して、共通情報発生回路3が発生するスクランブル鍵KSを暗号化する第1の暗号化手段としての暗号器6と、ワーク鍵KWと更新情報を暗号化する第2の暗号化手段としての暗号器8と、暗号器6により暗号化されたスクランブル鍵KS、並びに暗号器8により暗号化されたワーク鍵KWと更新情報を伝送する伝送手段としての送信回路9とを備えることを特徴とする。

30

【 0 0 1 1 】本発明の受信装置は、所定のタイミングで更新される暗号鍵としてのワーク鍵KWを用いて、伝送された情報、ワーク鍵KW、およびワーク鍵KWの更新情報を受信する受信装置において、更新情報を記憶する第1の記憶手段としての時間情報記憶部及びタイマ109と、時間情報記憶部及びタイマ109に記憶された更新情報に基づいて電源125を制御する制御手段としての電源制御部121と、更新情報に基づいて更新されるワーク鍵KWを記憶する第2の記憶手段としての暗号器104と、暗号復号器104に記憶されたワーク鍵KWに基づいて情報を復号する復号手段としての暗号復号器1

50

03とを備えることを特徴とする。

【 0 0 1 2 】更新情報が、ワーク鍵KWを更新する更新開始時刻を含む場合、時間情報記憶部及びタイマ109は、更新開始時刻に、電源125を一定時間オンするようにすることができる。

【 0 0 1 3 】更新情報が、ワーク鍵KWを更新する更新開始時刻及びワーク鍵KWの更新期間を含む場合、時間情報記憶部及びタイマ109は、更新開始時刻に電源125をオンさせるとともに、更新期間に対応する時間経過後に、電源125をオフさせるようにすることができる。

【 0 0 1 4 】更新情報が、ワーク鍵KWを更新する更新開始時刻及びワーク鍵KWの更新終了時刻を含む場合、時間情報記憶部及びタイマ109は、更新開始時刻に電源125をオンさせるとともに、更新終了時刻に電源125をオフさせるようにすることができる。

【 0 0 1 5 】

【作用】上記構成の送信装置では、暗号器6により暗号化されたスクランブル鍵KS、並びに暗号器8により暗号化されたワーク鍵KWと更新情報が、送信回路9により伝送路に伝送される。従って、無駄に電力を消費することなく、ワーク鍵KWを確実に更新させることが可能になる。

【 0 0 1 6 】上記構成の受信装置では、暗号復号器104は、ワーク鍵KWを更新毎に書き換えて記憶する。また、時間情報記憶部及びタイマ109は、更新情報を記憶する。時間情報記憶部及びタイマ109からの制御信号に基づいて電源制御部121が電源125を制御することで、簡単かつ確実に、ワーク鍵KWを効率的に更新することを可能とする。

【 0 0 1 7 】

【実施例】図1乃至図3は、本発明の送信装置と受信装置を応用した有料放送送信装置と受信装置の一実施例に係わり、図1は有料放送送信装置であるエンコーダの一実施例の要部の構成を示すブロック図、図2は図1のエンコーダに用いられる個別情報の一構成例を説明する説明図、図3は有料放送受信装置であるデコーダの一実施例の要部構成を示すブロック図である。

【 0 0 1 8 】図1のエンコーダにおいては、データ供給装置1が出力する転送すべきデータ（例えば新聞、雑誌等のキャラクタデータ）がスクランブラ2に供給され、スクランブルされるようになされている。共通情報発生回路3が発生する共通情報に含まれる。スクランブル鍵KSがPN信号発生器4に供給され、PN信号発生器4が発生したPN信号がスクランブル2に供給されている。共通情報発生回路3が出力するスクランブル鍵KSと、それに対応する番組番号等を含む共通情報は、暗号器6に供給され、個別情報発生回路5が出力する個別情報の内、ワーク鍵KWに対応して、暗号化されるようになされている。

【0019】また、個別情報発生回路5が出力する個別情報（図2を参照してご述するように、契約内容、ワーク鍵K_W、次回更新時間情報等を含む）は、暗号器8に供給され、マスタ鍵発生回路7が発生するマスタ鍵K_{mi}に対応して暗号化されるようになされている。

【0020】送信回路9は、スクランブラ2、暗号器6ならびに暗号器8より供給されるデータを合成し、アンテナ10を介して、例えば衛星に伝送するようになされている。

【0021】図2は、個別情報発生回路5が出力する個別情報の例を表している。この個別情報は、同図に示すように、符号化識別情報161（16ビット）、関連情報識別情報162（2ビット）、ユーザID163（32ビット）、ワーク鍵（K_W）164（32ビット）、ワーク鍵対象番組情報165（P_V、S_V、P_R：40ビット）、契約登録コード166（12ビット）、鍵有効期限情報167（11ビット）、個別情報送信予定日時情報168（10ビット）、改ざん検出情報169（16ビット）、その他の情報170（5ビット）から構成されていて、電気技術審議会の答申に基づいてい

る。

【0022】このように、共通情報は、各受信者に共通の情報を含んでいるが、個別情報は、個々の受信者毎に異なる情報を含んでいる。

【0023】次に、図1の実施例の動作について説明する。共通情報発生回路3が発生するスクランブル鍵K_Sは、PN信号発生器4に供給される。PN信号発生器4は、入力されるスクランブル鍵K_Sに対応してPN信号を発生し、スクランブラ2に供給する。スクランブラ2は、データ供給装置1より供給されるデータを、PN信号発生器4より入力されるPN信号に対応してスクランブルし、送信回路9に出力する。このスクランブル鍵K_Sは、比較的短い周期（例えば1秒毎）で変更（更新）される。

【0024】個別情報発生回路5が出力する個別情報のうち、ワーク鍵K_Wは、暗号器6に供給されている。暗号器6は、このワーク鍵K_Wに対応して、共通情報発生回路3より供給されるスクランブル鍵K_Sを暗号化し、送信回路9に出力する。このスクランブル鍵K_Sは、その更新周期（1秒間）の間に、少なくとも1回出力される。

【0025】また、暗号器8には、マスタ鍵発生回路7が発生するマスタ鍵K_{mi}が入力されており、暗号器8は、このマスタ鍵K_{mi}に対応して、個別情報発生回路5より入力される個別情報を暗号化し、送信回路9に出力する。

【0026】送信回路9は、スクランブラ2、暗号器6及び暗号器8より供給されるデータを合成し、アンテナ10を介して衛星に電波で伝送する。

【0027】このようにして、伝送された情報は、衛星

を介して図3に示すデコーダに電波で送信される。

【0028】本実施例のデコーダでは、図3に示すように、衛星より伝送された有料放送をBSチューナ101で受信する。BSチューナ101から出力されたビットストリームはバケット分離回路102に入力され、それぞれ暗号化されたデータ150、共通情報151（番組番号、スクランブル鍵K_S等）、個別情報152（契約内容、ワーク鍵K_W、次回更新時間情報等）の3種類のバケットに分離される。尚、101はBSチューナに限らず、CSチューナあるいはCATVの端末でも良い。

【0029】データ150はスクランブル鍵K_Sによりスクランブルされたデータであり、共通情報151は、ワーク鍵K_Wにより暗号化され、データ150の番組番号やスクランブル鍵K_S等から構成されている。また、図2に示すような個別情報152は、マスタ鍵K_{mi}により暗号化されている。

【0030】分離された個別情報152（ワーク鍵（K_W）164を含む）は、記憶部105に予め記憶されている各デコーダ個有のマスタ鍵（K_{mi}）131を用いて、暗号復号器104で復号され、そのうちのワーク鍵K_Wはそこに記憶される。そして、記憶されたワーク鍵（K_W）132が、暗号復号器103に入力され、これを用いて、暗号復号器103で、共通情報151（スクランブル信号K_Sを含む）が復号され、そのうちのスクランブル鍵（K_S）133が、PN信号発生器107に入力される。

【0031】条件比較器108は、暗号復号器104より供給される個別情報152内の契約条件を記憶すると共に、記憶した契約条件と、暗号復号器103から入力される共通情報151の内容とを比較し、契約条件と共通情報151の内容とが適合した場合、PN信号発生器107にイネーブル信号134を出力する。PN信号発生器107は、イネーブル信号134が入力されているとき、暗号復号器103からのスクランブル鍵K_S133を基にしてPN信号を生成し、デスクランブラ106に出力する。

【0032】そしてデスクランブラ106は、PN信号によりデータ150をデスクランブルして番組データ135を得て、サービスデコーダ120に出力する。サービスデコーダ120は番組データ135をデコードし、図示しないTV、専用端末等に出力する。

【0033】一方、暗号復号器104で復号された個別情報152内の更新情報としての個別情報送信予定日時情報168（次回の個部情報送信予定日時を表す）は、時間情報記憶部及びタイマ109に出力されており、時間情報記憶部及びタイマ109は、個別情報送信予定日時情報168を記憶し、タイマをセットする。この時間情報記憶部及びタイマ109は、記憶した次回の個別情報送信予定時刻になると、電源制御部121へ制御信号を出力し、電源制御部121はこの制御信号によりデコ

ーダの電源 1 2 5 をオンする。従って、デコーダは、更新時に、確実に動作状態となり、個別情報 1 5 2 を受信し、ワーク鍵 K W を更新し、暗号復号基 0 4 に記憶する。

【 0 0 3 4 】尚、電源オンの期間は、個別情報の送信期間が予め予測可能であるので、一定時間（例えば 1 時間）とし、その期間にワーク鍵 K W を更新し、暗号復号基 1 0 4 に記憶し、その後電源 1 2 5 をオフする。

【 0 0 3 5 】このように本実施例のデコーダによれば、時間情報記憶部及びタイマ 1 0 9 からの制御信号により電源制御部 1 2 1 が自動的に電源 1 2 5 をオンし、電源オンの状態で個別情報 1 5 2 を受信し、ワーク鍵 K W を更新し、暗号復号器 1 0 4 に記憶するので、簡単かつ確実に有料放送の個別情報を効率的に更新できる。

【 0 0 3 6 】尚、電源オンの制御は、上記実施例の方法（一定時間オン）に限らず、個別情報 1 5 2 内のワーク鍵更新時間情報として、個別情報送信予定日時情報 1 6 8 に、ワーク鍵更新開始時刻とこのワーク鍵更新開始時刻から電源をオンさせる継続時間とを設定し、デコーダの時間情報記憶部及びタイマ 1 0 9 によりワーク鍵更新開始時刻に電源をオンして、継続時間経過後に電源をオフすることで、ワーク鍵 K W を更新し、暗号復号器 1 0 4 に記憶するようにしても良い。

【 0 0 3 7 】この場合、上記効果に加え、個別情報に更新開始時刻と電源をオンさせる継続時間を設定することにより、加入者の増減やサービスの変化に伴う次の個別情報送信時間のばらつきに柔軟に対処することができる。

【 0 0 3 8 】また、電源オンの制御のその他の方法として、個別情報 1 5 2 内のワーク鍵更新時間情報として、ワーク鍵更新開始時刻とワーク鍵更新終了時刻を設定し、この 2 つの情報からデコーダの時間情報記憶部及びタイマ 1 0 9 により電源をオン／オフさせるようにしても良い。

【 0 0 3 9 】具体的な個別情報 1 5 2 内のワーク鍵更新開始時刻とワーク鍵更新終了時刻は、それぞれ、例えば、一般的にワーク鍵の更新サイクルは月一回程度と考え、送信予定日時の付加を考慮して、“日”に 5 ビット、“時刻”を 1 時間単位の設定として 5 ビット、合計 1 0 ビットを用いるように構成すれば良い。こうすることで、次の更新時刻が明確である場合（すなわち加入者の人数の急激な増加や選択する番組の変化がない場合）において、デコーダの電源をより効率的に制御することが可能となる。

【 0 0 4 0 】尚、図 3 において暗号復号に関する部分（図中破線内）は、セキュリティモジュールと呼ばれ、

最近では I C カード等にアルゴリズム及びワーク鍵 K W の記録部分を持たせることで、デコーダ本体と分離する傾向にあるが、この場合においても、個別情報の更新時間情報の更新を I C カード（セキュリティモジュール）に記録させることで同様な効果を得ることができる。

【 0 0 4 1 】また、上記実施例では、暗号鍵を 3 重としたが、4 重以上、あるいは 1 重、2 重でもよい。

【 0 0 4 2 】

【発明の効果】以上説明したように本発明の送信装置によれば、暗号鍵と更新情報を伝送するようにしたので、無駄に電力を消費することなく、暗号鍵を確実に更新させることが可能になる。

【 0 0 4 3 】また、本発明の受信装置によれば、暗号鍵を更新毎に書き換えて記憶すると共に、更新情報に基づき電源を制御するので、簡単かつ確実に、暗号鍵を効率的に更新することができるという効果がある。

【図面の簡単な説明】

【図 1】本発明の送信装置であるエンコーダの一実施例の要部の構成を示すブロック図である。

【図 2】図 1 のエンコーダに用いられる個別情報の一構成例を説明する説明図である。

【図 3】本発明の受信装置であるデコーダの一実施例の要部の構成を示すブロック図である。

【図 4】従来の有料放送の送信装置及び受信装置の構成を示すブロック図である。

【符号の説明】

- 1 データ供給装置
- 2 スクランプラ
- 3 共通情報発生回路
- 4 P N 信号発生器
- 5 個別情報発生回路
- 6 暗号器
- 7 マスタ鍵発生回路
- 8 暗号器
- 1 0 1 B S チューナ
- 1 0 2 パケット分離回路
- 1 0 3、1 0 4 暗号復号器
- 1 0 5 記憶部
- 1 0 6 デスクランブラ
- 1 0 7 P N 信号発生器
- 1 0 8 条件比較器
- 1 0 9 時間情報記憶部及びタイマ
- 1 2 0 サービスデコーダ
- 1 2 1 電源制御部
- 1 2 5 電源

【图 2】

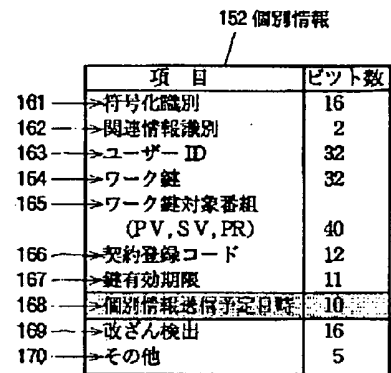
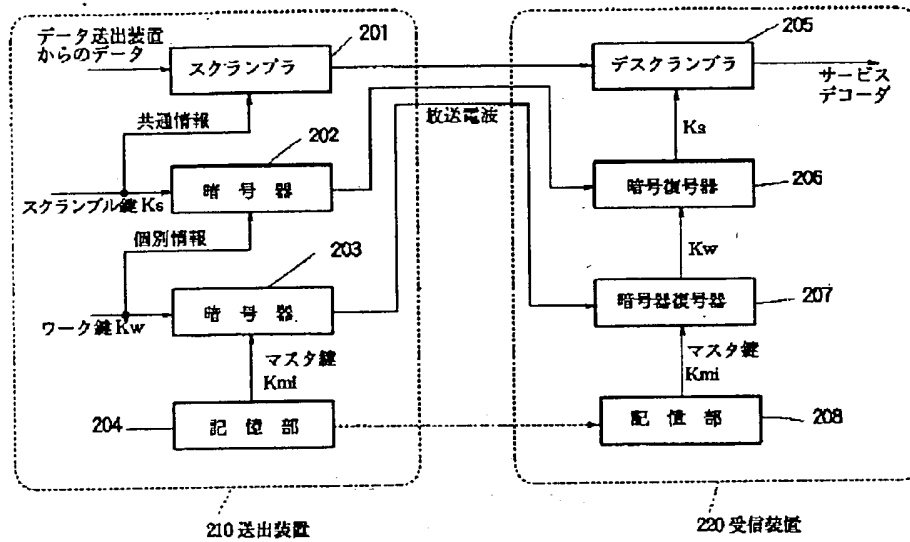


Figure 1 is a block diagram of a security module for a BS tuner. The diagram shows the flow of data and control signals between various components. A BS tuner (101) provides a bitstream (102) to a packet distributor (103). The distributor outputs data (150) to a descrambler (106) and common information (151) to a PN signal generator (107). The distributor also outputs individual information (152) to a PN signal generator (107), a PN signal generator (108), a condition comparator (109), and a time information storage unit (110). The PN signal generator (107) outputs a PN signal (135) to the descrambler (106). The PN signal generator (108) outputs a PN signal (134) to the condition comparator (109). The condition comparator (109) outputs a signal to the time information storage unit (110). The time information storage unit (110) outputs a signal to a power control unit (121). The power control unit (121) outputs a signal to a power source (125). The descrambler (106) outputs a signal to a service decoder (120), which outputs to a TV (TV等).

【図 4】



This Page Blank (uspto)